NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

SECTION III MANAGEMENT CONTROLS

Chapter 12 IT Security Risk Management

12.1 IT Security Risk Management Overview

12.1.1 NASA shall follow the NPR 8000.4, Risk Management Procedural Requirements, and include the requirements of NIST SP 800-30, Risk Management Guide for Information Technology System, for guidance on risk management processes. This chapter provides a high-level summary of risk management.

12.1.2 NASA accepts that complete avoidance of IT security risk is not cost-effective and may impact mission success. NASA management will ensure that IT security risks are assessed, analyzed, and mitigated to the point that residual risks are considered acceptable by management. Implicit to this concept is a "tailored" approach to IT security protection, in which information and functions of differing criticality are protected at different levels.

12.1.3 The IT security risk management program encompasses three processes: risk assessment, risk mitigation, and continuous risk management. These processes are continued throughout the system's life cycle from initiation to disposal and are performed at varying levels of complexity as the system matures.

12.2 Risk Management Process Requirements

12.2.1 The IT security risk management process shall:

a. Treat the NASA IT risk management process as an essential management function and not as a technical function primarily carried out by the IT experts who operate and manage the IT system.

b. Ensure that system risk analyses, risk mitigation alternatives analyses, and building a business case for the acquisition of appropriate security are coordinated and performed.

c. Ensure that all activities in the NASA risk management process address IT security for all information systems and applications.

d. Ensure that appropriate security is implemented to protect the system's information, including the implementation and maintenance of management, operational, and technical controls by working closely with system support personnel.

e. Define the potential impact on projects should a breach in security occur (i.e., a loss of confidentiality, integrity, or availability). Ensure that the system and information owners concur on the risks in accordance with NIST SP 800-30, which states "regardless of the method used to determine how sensitive an IT system and its data are, the System and Information Owners are the ones responsible for determining the impact level for their own system and information."

f. Determine the impact of security threats to the security objectives and then identify the proper measures that are required to protect against the unwanted disclosure of information, inadvertent or malicious corruption of data, or denial of authorized access to the system.

g. Balance both the operational and economic costs of measures to protect the IT systems and the information that support NASA missions. Assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

h. Ensure that all IT security risk management activities are performed whenever there is a significant change to the system or whenever a new risk is identified that will impact the current security posture.

i. Implement policies and procedures to cost-effectively manage risks to an acceptable impact level.

j. Annually test and evaluate a subset of information security controls and techniques to ensure that they are effectively implemented. Information system owners may define a subset of high impact controls to test annually. Further, the SAISO may publish a list of controls to be tested annually through a Directive letter.

k. Ensure that test results and resulting IT security recommendations are adopted as appropriate and that the choices are fully documented in the corresponding SSP.

l. Ensure that any unmitigated risks are documented in a POA&M.

12.2.2 Risk Assessment Process Requirements

12.2.2.1 NASA shall use NIST SP 800-30, Risk Management Guide for Information Technology System, Appendix B, Sample Risk Assessment Report Outline, which shall be summarized in the SSP and attached as an appendix to the SSP.

12.2.2.2 NASA shall use NIST SP 800-30, Risk Management Guide for Information Technology System, Appendix C, Sample Safeguard Implementation Plan Summary Table, which shall be attached as an appendix to the SSP.

12.2.2.3 Risk assessments shall be conducted based on system characterization as described in section 7.2, Categorization of Information.

12.2.2.4 The IT security risk assessment process shall:

a. Ensure that IT security risk assessment is an ongoing process and is conducted and integrated in the SDLC for all NASA IT systems and information resources.

b. Ensure that periodic assessments are performed throughout the SDLC of their information systems to determine the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Agency

c. Determine the appropriate levels of information security as described in section 7.2, Categorization of Information.

d. Ensure that a preliminary risk assessment is conducted for all information systems and applications, prior to system procurement, to estimate the level of impact associated with the planned information system.

e. Ensure that risk assessments and analyses for Agency master and subordinate IT Systems are conducted. Conduct risk assessments for subordinate IT systems based upon NIST's list of management controls, operational controls, and technical controls for the security category of the information system and any inherited controls from the master IT System. Focus of the risk assessment for the subordinate system will be on site-specific threats and vulnerabilities.

f. Ensure that a risk assessment summary report describing the information's security category and detailing the vulnerability/threat pairs, risk assessment results, and the potential impact is presented to the AO as part of the Certification and Accreditation Package.

g. Ensure that a IT security risk assessment team is assigned to facilitate and assist in analytical duties for risk assessment activities.

12.2.3 Risk Mitigation Process Requirements

12.2.3.1 NASA risk mitigation process shall:

a. Employ systematic methodologies to mitigate system IT security risk.

b. Prioritize, evaluate, and implement the appropriate cost-effective, risk-reducing controls recommended from the risk assessment process.

c. Ensure that test results and the resulting IT security recommendations are adopted as appropriate and that the choices are fully documented in the corresponding SSP.

d. Provide a record showing that the security controls were verified or tested, who verified or tested the controls, and if the verification or testing results were acceptable or unacceptable.

e. Provide the justification for any security controls that are not appropriate for the system in the Security Controls Assessment Table.

12.2.4 NASA Continuous Risk Management Process

12.2.4.1 NASA shall employ continuous a risk management process to:

a. Ensure that programs and projects integrate IT security risk management as defined in NIST SP 800-30, Risk Management Guide for Information Technology System, with the processes and procedures defined in NPR 7120.5, NASA Program and Project Management Process and Requirements, and NPR 8000.4, Risk Management Procedural Requirements.

b. Ensure that IT security risk assessment is an ongoing process and that risk management is conducted and integrated in the SDLC for all NASA IT systems and information resources in support of the NASA missions.

12.3 Additional IT Security Risk Management References

a. NIST SP 800-30, Risk Management Guide for Information Technology System.

b. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information.

c. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

d. NPR 8000.4, Risk Management Procedural Requirements.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS